

백서

# 마이크로세그멘테이션의 주요 사용 사례 탐색

작성자: John Grady, Enterprise Strategy Group 수석 애널리스트

2023년 1월

Enterprise Strategy Group 백서는 Akamai 의 의뢰를 받아 TechTarget, Inc.의 라이선스 하에 배포되었습니다.

## 목차

요약 보고서.....	3
추진력을 얻고 있는 제로 트러스트, 그러나 여전히 중요한 명확한 우선순위 수립의 문제.....	3
현재 제로 트러스트 모델 지원에서 활용도가 낮은 마이크로세그멘테이션.....	5
마이크로세그멘테이션의 주요 사용 사례 .....	6
위협 방지.....	7
비즈니스 전반의 효율성 향상.....	7
제로 트러스트 세그멘테이션.....	8
마이크로세그멘테이션에 대한 Akamai 의 접근 방식 .....	8
결론.....	9

## 요약 보고서

제로 트러스트는 사이버 보안 업계에서 보편화되어 가고 있습니다. 그러나 이니셔티브의 범위와 전략에서 가장 중요한 요소가 무엇인지에 대한 상충되는 견해 때문에 어디서부터 시작해야 할지, 프레임워크를 가장 잘 지원하는 툴은 무엇인지 혼란을 겪기도 합니다. 제로 트러스트의 구현 경로는 다양합니다. 제로 트러스트 전략은 궁극적으로 리소스와 기업이 서로 통신할 수 있도록 보장하는 방식을 기반으로 마이크로세그멘테이션의 중요성을 강조하고 있으며, 정책에서 명시적으로 허용하는 경우에만 서로 통신할 수 있도록 합니다.

마이크로세그멘테이션 툴의 사용은 현재 다소 제한적이지만, 제로 트러스트에 대한 마이크로세그멘테이션의 중요성과 다양한 사용 사례에 대한 적용 가능성에 대한 인식은 앞으로 크게 높아질 것입니다. 기업이 위협 방지, 비즈니스 전반에서 효율성 향상 또는 전반적인 보안 접근 방식의 최신화를 위해 제로 트러스트를 고려하고 있다면 마이크로세그멘테이션이 도움이 될 수 있습니다. 특히, 마이크로세그멘테이션을 위한 Akamai의 소프트웨어 기반 및 인공지능 지원 접근 방식은 정밀한 가시성을 제공하며, 기업이 측면 이동을 방지하고 랜섬웨어 공격을 차단하며 제로 트러스트 원칙을 모든 환경에 일관되게 적용할 수 있도록 합니다.

**기업이 위협 방지, 비즈니스 전반에서 효율성 향상 또는 전반적인 보안 접근 방식의 최신화를 위해 제로 트러스트를 고려하고 있다면 마이크로세그멘테이션이 도움이 될 수 있습니다.**

## 추진력을 얻고 있는 제로 트러스트, 그러나 여전히 중요한 명확한 우선순위 수립의 문제

리소스가 클라우드로 이동하고, 디지털 비즈니스 모델이 자리를 잡아가며 사용자가 점점 더 분산됨에 따라 기업 환경은 점점 복잡해지고 있습니다. 공격자들이 방어 체계의 허점을 뚫고 랜섬웨어 공격을 시도하거나 고객 정보를 훔치거나 민감한 지적 재산을 유출하려고 하기 때문에 이러한 변화는 본질적으로 사이버 보안 팀의 업무를 더욱 어렵게 만듭니다. 하지만 과도하게 허용적인 경계 기반 제어를 기반으로 하는 기존의 보안 접근 방식으로는 더 이상 이러한 현실을 해결할 수 없으므로 보안 팀은 전략을 재평가해야 합니다. 또한 공격이 보다 정교해지고 횡수도 늘어남에 따라 보안 팀이 모든 잠재적인 위협을 확인하고 이를 해결하며 패치하는 것은 불가능합니다.

이러한 문제가 생기자 많은 이들이 제로 트러스트에 주목하게 되었습니다. 제로 트러스트 전략이 완전히 새로운 개념은 아니지만, 사이버 보안과 관련해 보다 역동적이면서도 최소한의 권한으로 리스크 기반 접근 방식을 활용하기 때문에 기업들이 상당한 관심을 보이고 있습니다. 제로 트러스트 접근 방식은 환경에서 암묵적 신뢰를 없애고 모든 디지털 상호 작용을 지속적으로 검증합니다. 따라서 제로 트러스트 방식을 활용하면 보안 팀이 리소스, 사용자, 디바이스의 안전을 확보할 수 있습니다. 그러나 제로 트러스트의 광범위한 적용 가능성과 제로 트러스트에 대한 상충되는 견해 및 정의 때문에 혼란이 야기되며 기업이 출발점을 파악하기 어려울 수 있습니다.

기업의 우선순위와 원하는 결과를 평가하고 파악하면 집중해야 할 범위를 좁히고 제로 트러스트 이니셔티브를 시작할 위치를 결정하는 데 도움이 됩니다. 기업이 제로 트러스트를 추진하는 비즈니스 동기는 다양합니다 (그림 1 참조).<sup>1</sup> 가장 일반적인 목표는 사이버 보안의

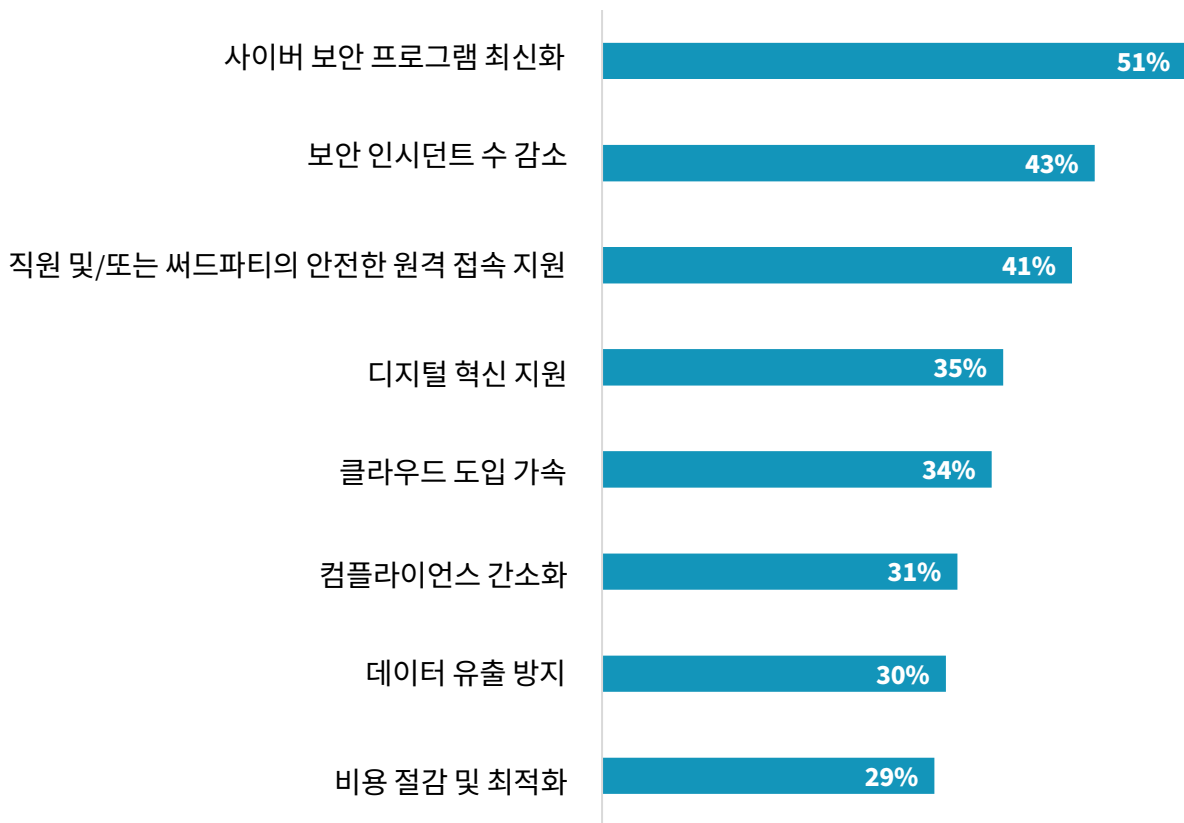
**제로 트러스트 전략은 리소스와 기업이 서로 통신할 수 있도록 보장하는 방식을 기반으로 정책에서 명시적으로 허용하는 경우에만 통신을 허용합니다.**

<sup>1</sup> 출처: Enterprise Strategy Group 설문조사 결과, [The State of Zero Trust Security Strategies](#), 2021년 5월.

최신화입니다(응답자의 51%). 이러한 사고방식은 바이든(Biden) 행정부가 발표한 사이버 보안에 관한 행정 명령을 통해 미국 연방 정부가 최신화 요건으로 제로 트러스트 아키텍처를 규정하며 더욱 강조되었습니다. 이 행정 명령은 민간 부문을 직접 대상으로 하지는 않지만, 연방 정부 외부의 보안 팀에 방향을 제시하는 지침이 될 수 있습니다. 제로 트러스트를 위한 다른 전략적 목표로는 디지털 혁신 지원(35%)과 클라우드 도입이 가속(34%)이 있습니다. 이러한 동기는 많은 기업에서 보안 팀이 자산 보호 외에도 비즈니스를 지원하는 데 부가적인 도움이 되어야 한다는 기대치를 강조합니다. 보안 인시던트 감소(43%), 안전한 원격 접속 지원(41%), 컴플라이언스 간소화(31%), 데이터 유출 방지(30%) 등도 일반적인 전술적 목표입니다.

### 그림 1. 제로 트러스트를 위한 동인

귀사에서 제로 트러스트 전략을 도입했거나 고려 중일 경우, 그와 관련하여 가장 중요한 비즈니스 동기는 무엇입니까? (응답자 비율, N=421, 3개 응답 허용)



출처: TechTarget, Inc.의 사업부, Enterprise Strategy Group

제로 트러스트 프로젝트가 초기에 집중해야 하는 범위를 좁히면 보안 팀이 전략 지원에 필요한 톨을 파악하는 데 도움이 될 수 있습니다. 예를 들어, 직원과 써드파티를 위한 안전한 원격 접속을 개선하는 것이 목표라면, 대부분의 경우 ZTNA (Zero Trust Network Access)에 주목할 것입니다. MFA(Multifactor Authentication)와 같은 ID 톨도 이러한 시나리오에 활용할 수 있습니다. 그러나 비즈니스 동기에 따라 기술 요구 사항을 명확하게 규정하지 않거나, 많은 기업이 범위를 좁힌 후 여러 가지 목표에 집중하는 경우도 있습니다. 이러한 상황에서는 기업이 다양한 사용 사례와 목표를 지원할 수 있는 톨과 그 방법을 파악하는 것이 중요합니다.

## 현재 제로 트러스트 모델 지원에서 활용도가 낮은 마이크로세그멘테이션

제로 트러스트의 구현 경로는 다양합니다. 제로 트러스트 전략은 궁극적으로 리소스와 기업이 서로 통신할 수 있도록 보장하는 방식을 기반으로 정책에서 명시적으로 허용하는 경우에만 통신을 허용합니다. 즉, 어떤 기업에서든 제로 트러스트 철학의 핵심은 성공한 공격의 영향을 제한할 수 있도록 자산을 적절히 세그멘테이션하는 능력에 있습니다. 이는 사이버 보안 최신화와 같은 광범위한 목표나 데이터 유출 방지와 같은 좁은 범위의 개별 목표에 모두 적용될 수 있습니다.

그러나 현재 환경에서는 일반적으로 대략적인 수준의 세그멘테이션으로는 충분하지 않으며, 기업 자산을 적절히 보호하기 위해서는 보다 정밀한 마이크로세그멘테이션이 필요합니다. 최신 애플리케이션 아키텍처는 여러 서버 인스턴스와 경우에 따라 멀티 클라우드 환경에 분산된 워크로드를 사용하는 경우가 많습니다. 위치에 기반해 리소스를 세그멘테이션하는 방식은 시대에 뒤떨어지고 있으며, 보안 팀이 현재 직면하고 있는 과제를 해결하지 못합니다.

지금까지 기업은 마이크로세그멘테이션 툴의 도입을 다소 주저해 왔습니다. TechTarget 의 ESG(Enterprise Strategy Group) 연구에 따르면 28%의 기업이 마이크로세그멘테이션이 너무 복잡하다고 생각하는 것으로 나타났습니다. 그러나 이는 주로 보안 팀이 마이크로세그멘테이션에 잘못된 툴을 사용하기 때문일 수 있습니다. ESG 연구에 따르면 기업의 55%가 마이크로세그멘테이션을 위한 툴로 방화벽과 같은 인프라 기반 툴을 사용한다고 보고한 반면, 호스트 기반 툴을 사용하는 비율은 8%에 그쳤습니다.<sup>2</sup> 방화벽은 마이크로세그멘테이션을 성공적으로 수행하는 데 필요한 정밀한 정책을 적용할 수 없습니다. 또한 이 툴이 애플리케이션 워크로드에 대해 제공하는 가시성은 제한적이어서 온프레미스 및 클라우드 위치에서 환경의 모든 측면을 일관되게 해결하기 어렵습니다.

이러한 이유로 마이크로세그멘테이션의 활용도는 낮은 상황입니다. ESG 연구에 따르면, 제로 트러스트가 중요함에도 불구하고 현재 마이크로세그멘테이션을 사용하는 기업은 36%에 불과합니다(그림 2 참조). 다행히 많은 기업이 마이크로세그멘테이션을 사용하느냐에 따라 방어에 상당한 격차가 있음을 인식하고 있습니다. 그 결과 91%는 24 개월 후 마이크로세그멘테이션을 사용할 예정인 것으로 나타났습니다.<sup>3</sup> 마이크로세그멘테이션은 궁극적으로 물리적 네트워크, 가상 네트워크, 클라우드 네트워크를 외부와 내부 위협으로부터 보호함으로써 제로 트러스트의 주요 이점을 구체화하고 강화하며, 제로 트러스트 전략의 핵심 구성요소가 되어야 합니다.

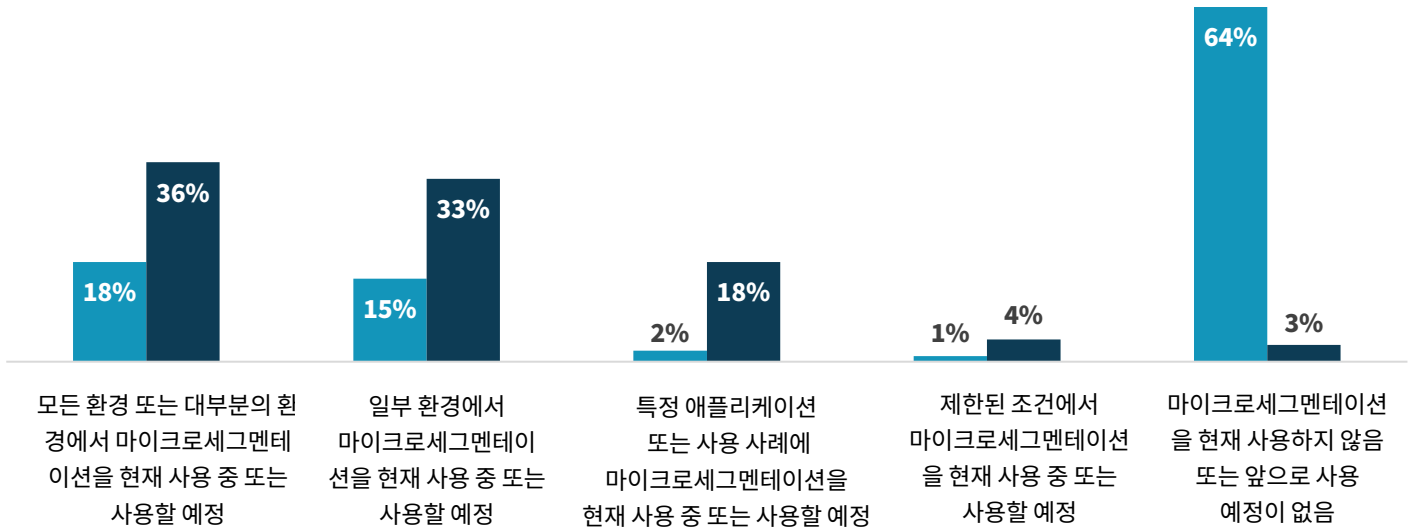
<sup>2</sup> 출처: Enterprise Strategy Group 전체 설문조사 결과, [Network Security Trends in Hybrid Cloud Environments](#), 2021 년 12 월.

<sup>3</sup> 동일 보고서

## 그림 2. 마이크로세그멘테이션 도입

다음 중 귀사의 마이크로세그멘테이션 활용 방안을 가장 잘 나타내는 항목은 무엇입니까?  
(응답자 비율, N=255)

■ 현재 ■ 지금부터 24 개월 후



출처: TechTarget, Inc.의 사업부, Enterprise Strategy Group

## 마이크로세그멘테이션의 주요 사용 사례

마이크로세그멘테이션은 다양한 제로 트러스트 사용 사례에 광범위하게 적용할 수 있기 때문에 그 어느 때보다도 더 강조되고 있습니다. 하지만 무엇보다 중요한 점은 마이크로세그멘테이션이 제로 트러스트를 향한 기업의 여정에서 좋은 출발점이 된다는 것입니다. 특히 워크로드 및 기업 관계에 전반에 걸쳐 매우 정밀한 가시성을 제공하는 솔루션을 활용한다면 마이크로세그멘테이션을 통해 기업의 가장 중요한 자산을 보호할 수 있기 때문입니다. 트래픽 흐름과 의존성의 기준을 발전시키는 것은 비즈니스를 중단하지 않고 암묵적 신뢰를 없애기 위한 첫 단계로, 제로 트러스트를 위한 노력의 토대가 됩니다. 이러한 접근 방식을 통해 보안 팀은 가장 중요한 자산을 신속하게 보호함으로써 제로 트러스트를 구현하는 동안 유출이 발생할 경우 미치는 영향을 제한할 수 있습니다. 보안 팀은 이러한 확신을 바탕으로 마이크로세그멘테이션이 지원하는 다른 사용 사례에도 관심을 돌릴 수 있습니다.

## 위협 방지

제로 트러스트는 보안 프레임워크이며, 보안의 목표는 사이버 위협으로부터 기업을 보호하는 것입니다. 따라서 마이크로세그멘테이션의 주요 사용 사례 중 일부는 위협을 방지하고 기업 리소스에 미치는 영향을 제한하는 데 중점을 두고 있습니다.

- 중요 자산의 링펜싱.** 보안 팀은 보호 우선순위를 결정할 때 리스크의 가중치를 판단하고 균형을 맞춰야 합니다. 규제된 고객 정보, 지적 재산 또는 기타 민감한 정보를 포함하는 높은 가치의 애플리케이션에 대해서는 시스템이 감염될 경우 잠재적 영향을 고려해 더욱 주의를 기울이고 보안 제어를 강화해야 합니다. 보안 팀은 마이크로세그멘테이션을 통해 이러한 애플리케이션과 애플리케이션을 구성하는 워크로드를 나머지 인프라와 완전히 분리할 수 있습니다.
- 측면 이동 제한.** 제로 트러스트는 기본적으로 공격자가 기업 네트워크에 접속할 수 있다고 가정하는 ‘유출 가정’의 원칙에 기반해 작동합니다. 기존의 엔드포인트, 서버, 클라우드 리소스, 심지어 스마트 디바이스의 무분별한 확산으로 침입은 불가피합니다. 따라서 마이크로세그멘테이션을 통해 잠재적인 공격의 피해 반경을 제한하면 네트워크에서 공격자의 측면 이동을 차단할 수 있습니다.
- 위협 탐지 및 대응.** 일단 공격이 발생했다면, 그 다음은 시간이 핵심입니다. 마이크로세그멘테이션 툴은 애플리케이션 관계를 기반으로 잠재적인 공격 경로를 신속하게 파악하고, 공격 중에 공격자가 사용하는 포트를 차단하며, 영향받는 시스템을 네트워크의 나머지 부분과 신속하게 격리함으로써 보안 팀이 빠르고 효과적으로 대응할 수 있도록 지원합니다. 여기에는 초기 진입 지점에 대한 공격도 포함됩니다.

## 랜섬웨어로부터 보호

랜섬웨어의 지속적인 확산과 이러한 공격의 영향으로 인한 문제는 이사회까지는 아니더라도 경영진에게 보고됩니다. 랜섬웨어에 대비하려면 강력한 보안뿐만 아니라 뛰어난 데이터 보호 및 인시던트 대응 능력도 필요하지만, 기업은 마이크로세그멘테이션을 통해 공격에 맞설 수 있는 확실한 토대를 마련할 수 있습니다. 공격자는 종종 공격 과정에서 민감한 정보와 시스템을 공격하는데, 이는 환경에 침투하고 정찰에 상당한 시간을 들인 후에만 가능합니다.

마이크로세그멘테이션을 사용해 중요 자산을 링펜싱하고 측면 이동을 제한하면, 공격자가 환경 전체에서 이동할 수 있는 자유가 줄어듭니다. 또한 랜섬웨어 공격이 발견될 경우 마이크로세그멘테이션을 사용하는 기업은 공격자가 이용하는 통신 경로를 신속하게 차단하고 감염된 서버를 격리해 공격이 더 이상 확산되지 않도록 막을 수 있습니다.

## 비즈니스 전반의 효율성 향상

보안 팀의 첫 번째 목표는 환경 보호이지만, 오늘날에는 이러한 경우에도 비즈니스 효율성에 영향을 주지 않도록 의무화하고 있습니다. 보안 팀이 실질적으로 동료를 지원할 수 있다면 비즈니스의 효율성도 증가할 것입니다. 다양한 도움을 줄 수 있지만 그중에서도 가장 일반적인 몇 가지만 살펴보겠습니다.

- 클라우드 도입 지원.** 클라우드로의 전환은 전혀 새로운 것이 아니지만, 클라우드 보안은 여전히 많은 기업에서 가장 중요한 문제입니다. 이러한 문제는 서비스형 인프라 플랫폼의 기본 보안 제어 기능에 익숙하지 않다는 점과 하이브리드 클라우드 환경의 일관되지 않은 보안이 원인일 수 있습니다. 마이크로세그멘테이션은 환경의 모든 측면에서 제어 기능을 적용할 수 있고 하이브리드 클라우드 시나리오에서 더 뛰어난 보안 일관성을 제공하므로 기업이 보안 체계를 더욱 신뢰할 수 있습니다.
- 애플리케이션 최신화 지원.** 클라우드로의 전환 외에도 컨테이너와 같은 최신 애플리케이션 아키텍처가 매우 빠르게 도입되고 있습니다. 이러한 모델을 통해 애플리케이션 팀은 이전보다 빠르게 애플리케이션을 설계, 구축,



배포할 수 있습니다. 개발자의 업무를 방해하지 않고 이러한 리소스를 보호하는 툴은 비즈니스에 긍정적인 영향을 줍니다. 컨테이너 환경의 트래픽 흐름에 대한 가시성을 제공하고 컨테이너가 온라인 상태가 되거나 이동할 때 자동으로 세그멘테이션 정책을 적용하는 마이크로세그멘테이션 툴은 개발 팀이 애플리케이션의 보안을 유지하는데 도움을 줍니다.

- 컴플라이언스 간소화.** 기업은 규제 문제에 점점 더 많은 관심과 시간, 예산을 들이고 있습니다. 데이터 프라이버시 침해 또는 개인 식별 정보 손실과 같은 잠재적인 문제의 영향을 제한하기 위해 보안 리스크를 최대한 격리하면 관련 프로세스의 부담을 줄일 수 있습니다. 마이크로세그멘테이션을 구축하면 컴플라이언스 요구 사항에 종속된 시스템을 나머지 환경으로부터 격리할 수 있으므로 보안 팀의 부담을 줄일 수 있습니다.

## 제로 트러스트 세그멘테이션

마이크로세그멘테이션의 가장 큰 이점은 목표로 하는 사용 사례에 초점을 맞출 때 기업에 즉각적인 가치를 제공할 수 있다는 점입니다. 먼저 거부 목록, 중요한 애플리케이션의 링펜싱, 환경 세그멘테이션, 기타 복잡성이 낮은 정책부터 시작해도 상대적으로 간편한 방식으로 빠르게 가치를 제공하므로 많은 경우에 매우 유용한 옵션입니다. 전사적으로 한 번에 완벽한 마이크로세그멘테이션 전략을 구축하는 기업은 거의 없습니다. 그러나 제로 트러스트 이니셔티브의 범위 내에서 마이크로세그멘테이션이 환경 전체에 더 광범위하게 배포됨에 따라 많은 기업이 제로 트러스트 세그멘테이션에 접근하기 시작할 것입니다. 이를 통해 기업은 트래픽 흐름에 대한 포괄적이고 정밀한 가시성을 유지하고, 가장 민감한 자산을 보호하며, 측면 이동을 방지하고, 위협에 신속하게 대응하는 동시에 비즈니스의 효율성을 높이면서 이전에 언급한 긍정적인 목표와 사용 사례를 모두 지원할 수 있습니다. 아직은 이를 출발점으로 삼을 수 있는 마이크로세그멘테이션 프로젝트가 많지 않지만, 앞으로는 이를 목표로 삼아야 합니다.

## 마이크로세그멘테이션에 대한 Akamai 의 접근 방식

기업은 마이크로세그멘테이션이 제로 트러스트의 핵심이며, 위협 탐지 및 대응, ID, 데이터 보안 등을 지원하는 기타 기술이 필요한 다른 주요 구성요소도 있다는 점을 명심해야 합니다. 기술 벤더를 평가하고 선정할 후 함께 협력하는 과정은 세부적 분석이 필요한 체계적인 프로세스로, 이 과정은 기업이 사이버 보안 목표를 달성할 것인지, 아니면 비용, 시간, 인력 리소스를 낭비할 것인지를 좌우할 수 있습니다. 따라서 광범위한 통합 및 신호 공유 기능을 제공하는 마이크로세그멘테이션 툴을 고려한다면, 마이크로세그멘테이션을 뛰어넘어 제로 트러스트 전략을 발전시키는 동시에 운영 복잡성을 줄일 수 있습니다.

**Akamai Guardicore Segmentation 솔루션은 마이크로세그멘테이션을 위한 소프트웨어 기반 접근 방식이며, 전체 디지털 환경에서 공격자의 측면 이동을 차단하기 위해 설계되었습니다.**

네트워크 인프라 분야에서 오랜 세월 자리를 굳게 다져 온 Akamai 는 [솔루션 포트폴리오의 핵심 기능으로 마이크로세그멘테이션과 제로 트러스트](#) 솔루션을 제공합니다. Akamai 는 잠재적인 사이버 보안 문제를 찾아내 해결한 경험을 토대로 온프레미스 및 클라우드 환경 모두에서 기업의 인프라 요구 사항에 관한 지식 기반을 구축했습니다.

[Akamai Guardicore Segmentation](#) 은 마이크로세그멘테이션을 위한 소프트웨어 기반 접근 방식이며, 전체 디지털 환경에서 공격자의 측면 이동을 차단하기 위해 설계되었습니다. 또한 정밀한 가시성을 바탕으로 네트워크 수준에서 제로 트러스트 원칙을 적용함으로써 기업이 물리적 환경과 가상 환경 내 활동과 이동을 시각화할 수 있도록 지원합니다. Akamai 의 인공지능 기반 세그멘테이션 프레임워크는 통합 템플릿을 사용해 랜섬웨어, 엔드포인트 기반 공격, 원격 근무 인력 기반 공격과 같은 침입을 탐지하고 차단합니다. 그리고 베어 메탈 서버, 가상 머신, 컨테이너, IoT 디바이스, 클라우드 인스턴스를 비롯한 다양한 플랫폼에서 사용할 수 있습니다.



Akamai Guardicore Segmentation 은 에이전트 기반 센서, 네트워크 기반 데이터 수집, 가상 프라이빗 클라우드 흐름 로그, 에이전트 없는 기능을 촉진하는 통합 등 여러 가지 방법으로 기본 인프라에 대한 광범위한 데이터를 수집합니다. 관리자는 동적 매핑을 통해 대략적 수준에서 활동에 대한 포괄적인 가시성을 확보할 수 있습니다. 기업 네트워킹 환경에서 쌓은 Akamai 의 경험을 바탕으로 Akamai Guardicore Segmentation 은 트래픽 병목 현상의 원인을 식별하고 우회하는 기업의 확장성과 일관된 성능을 제공하도록 설계되었습니다.

## 결론


마이크로세그멘테이션은 새로운 기술이 아닙니다. 그러나 시대를 앞서간 선구적인 기술입니다. 최신 하이브리드, 멀티 클라우드 환경을 보안하고, 특히 제로 트러스트 전략을 운용하는 데 있어 마이크로세그멘테이션의 중요성은 아무리 강조해도 지나치지 않습니다. 마이크로세그멘테이션은 미션 크리티컬 및 비즈니스 크리티컬 사용 사례에서 제로 트러스트를 실현하는 데 필요한 유연성, 민첩성, 효율성을 제공함으로써 중요 인프라와 지적 재산부터 ID 및 자격 증명에 이르는 모든 것을 보호합니다. 네트워크 인프라, 세그멘테이션, 마이크로세그멘테이션에 대한 Akamai 의 경험은 마이크로세그멘테이션 툴과 원칙을 기반으로 구축된 안전한 인프라를 계획, 구축, 배포, 관리할 수 있도록 지원합니다.

모든 제품명, 로고, 브랜드 및 상표는 해당 소유주의 자산입니다. 이 간행물에 포함된 정보는 TechTarget, Inc.가 신뢰할 수 있다고 간주하는 출처를 통해 수집했지만 TechTarget, Inc.에서 보증하지는 않습니다. 이 간행물에는 TechTarget, Inc.의 의견이 포함되어 있으며, 해당 의견은 변경될 수 있습니다. 이 간행물에는 현재 사용 가능한 정보를 고려한 TechTarget, Inc.의 가정 및 기대를 나타내는 예측, 추정, 예측의 성격을 띤 기타 진술 등이 포함될 수 있습니다. 이러한 예측은 업계 동향을 기반으로 하며 여러 변수와 불확실성을 포함합니다. 따라서 TechTarget, Inc.는 여기에 포함된 특정 예측, 추정 또는 예측성 진술의 정확성에 대해 어떠한 보증도 하지 않습니다.


발행물의 저작권은 TechTarget, Inc.에 있습니다. 본 발행물의 전부 또는 일부를 TechTarget, Inc.의 명시적 동의 없이 인쇄물, 전자 형식 또는 기타 형식으로 수령 권한이 없는 사람을 대상으로 복제 및 재배포하는 행위는 미 저작권법 위반에 해당하며, 민사상 손해 배상 및 형사 처벌(해당하는 경우)을 받게 됩니다. 궁금한 사항은 Client Relations([cr@esg-global.com](mailto:cr@esg-global.com))로 문의하십시오.



Enterprise Strategy Group은 글로벌 기술 커뮤니티에 마켓 인텔리전스, 실행 가능한 통찰력 및 GTM(Go to Market) 콘텐츠 서비스를 제공하는 통합 기술 분석, 연구 및 전략 회사입니다.

 [www.esg-global.com](http://www.esg-global.com)

 [contact@esg-global.com](mailto:contact@esg-global.com)

 508.482.0188